

Cyber Policing in the North West

Regional and Local Co-Ordination

**Contents**

Foreword

[Introduction 1](#_Toc397588339)

[Cyber Policing in the North West 2](#_Toc397588340)

[Defining Cybercrime 3](#_Toc397588341)

[Survey Findings 4](#_Toc397588342)

[Experience of Cybercrime 4](#_Toc397588343)

[Perceptions of cybercrime 5](#_Toc397588344)

[Cyber Pledge Analysis 7](#_Toc397588345)

[Working Group Findings 9](#_Toc397588346)

[Monitoring and Measuring Cyber Criminal Activity 9](#_Toc397588347)

[Defining Local and Regional Capacity 10](#_Toc397588348)

[Regional Support 12](#_Toc397588349)

[Intelligence Led Cyberpolicing Innovation Ecosystem 14](#_Toc397588350)

[Conclusion 16](#_Toc397588351)

[Appendix A - Pledges 18](#_Toc397588352)

[Authors 19](#_Toc397588353)

[References 20](#_Toc397588354)

Cybercrime is an insidious and growing threat within our society with the potential to cause significant personal and economic harm. It is vital that as law enforcement agencies we lead the way in responding to this threat taking the best of our traditional sound policing approaches and combining them with innovations in science, technology and industry.

This report marks the start of an on going and interesting discussion on how those agencies tasked with protecting the public and their use of cyberspace can respond to the growing threat that is cybercrime. It is important for several reasons, firstly the exploration of inter-force collaboration and how that might be supported by regional organisation is vital in order to combat the inherently non-geographical nature of cybercrime. Secondly, it presents new approaches and the wider sets of partners, such as academia and industry, that can be brought in to facilitate agile policing to tackle the rapidly evolving nature of cybercrime. Finally, it demonstrates the potential that such wide and varied collaborations have through the innovative ideas generated during the workshop.

I am therefore delighted by the contents of this report and the outcomes from the workshop in stimulating debate and illuminating new opportunities in the future. I would like to thank both TITAN and Lancaster University for hosting the workshop and the production of this report.

Introduction

In recent year the advent of digital technology has given rise to a new range of capabilities and opportunities for the average citizen in the UK. According to the Office of National Statistics (2013) the average weekly spend online was £586.6 million in July 2013, an increase of almost 11 percent compared with July 2012 (ONS, 2013).

However, these new capabilities have also afforded the criminal new opportunities to extend their reach, target high volumes and broader potential victim communities and provide new approaches to criminal enterprise. Knowledge about the level and nature of cybercrime activity in the UK has mostly come from the Commercial Victimisation Surveys. The survey has so far had four sweeps – in 1999, 2002 and a ten-year gap to 2012 and a further survey in 2013. A further survey in 2014 is planned, which will allow meaningful changes over time to be assessed. The 2013 CVS shows there were 269,000 incidents of online crime against businesses in total in the 4 industry sectors covered by the survey in the 12 months prior to interview, up from 180,000 in 2012. Cybercrime therefore presents new and unique challenges to law enforcement, the commercial sector and the public.

Despite its relative infancy cybercrime is now considered a major criminal activity by governments and one of the fastest growing and continually adapting crimes (Bodeau *et al.,* 2010). Since 2010 the UK government has placed tackling cybercrime as one of their highest priorities with Maguire and Dowling (2013a) noting its ‘Tier One’ threat status in the national security strategy (HMSO, 2010) and that £860 million of public funding has been set aside as part of a five-year National Cyber Security Programme. In order to tackle this, the newly formed National Crime Agency (NCA) formed the National Cybercrime Unit (NCCU) on the 7th October 2013. In order to achieve this the NCA absorbed approximately 80% of the existing cyber capability that was then operating in law enforcement. This includes the specialist Police Central e-crimes Unit (PCeU) and their existing regional capability. In addition to this consolidation, Regional Organised Crime Units (ROCUs) Were tasked to provide a regional E-crime capability that mirrors the terms of reference previously held by PCeU but Tailored to meet regional requirements as outlined in the ACPO ROCU Core Capabilities Document (Credon Nov 2012). Coupled with this the Strategic Policing Requirement (Home Office July 2012) requires Forces to provide and maintain training, specialist skills, equipment and the capability to conduct complex cyber investigations whilst having regard to connecting resources locally, inter force and nationally.

In response, TITAN – The North Wests ROCU- held a planning event facilitated by Security Lancaster at Lancaster University to take the first steps in the regions response to these growing demands. The workshop included representatives from the NCA, NCCU and the six forces that make up the North West Region. In addition, to members of Law enforcement, the workshop had representatives from academia, the commercial sector and selected individuals from cyber security organisations. Providing insightful presentations and discussion sessions, the goal of the event was to improve the collective understanding of the cyber threat and how the regional forces might be able to respond in a constructive and pro-active fashion by utilising currently embedded expertise and relationships with external organisations.

This report presents the findings of the workshop.

# Cyber Policing in the North West

Cybercrime prevention, detection and investigation are a priority for the Chief Constables and Police and Crime Commissioners for all of the North West forces. The North West police region encompasses the police forces of Cheshire, Cumbria, Greater Manchester, Lancashire, Merseyside and North Wales.

The forces have Cybercrime Strategies, which specifically address how they will tackle the threat posed to their communities and businesses by cybercrime. Without exception forces are examining their cybercrime capability and anticipate that it will be enhanced in the near future. Each of the six North West forces has a dedicated unit that specialises in the examination of computers and other digital devices. The titles of the units varies but commonly are referred to as Hi-Tech Crime or E-Forensics units. The primary function of these units is to forensically examine, extract and analyse data from computers and digital media. Whilst each force is experiencing challenges posed by the number of forensic submissions it receives against a back drop of budget cuts and constraints, all have appropriately trained staff and equipment which enables them to deal effectively with digital forensic examination.

All North West forces have an Internet Investigation capability; each force has appropriately trained staff and IT that enables the force to conduct open source research and conduct online investigations. Good practice is evident in Cheshire Constabulary, a force that has enhanced its IT infrastructure to greatly increase its capacity to conduct open source research.

The College of Policing has invested significantly in designing and delivering bespoke cybercrime training. E-Learning modules providing cybercrime training for first responders and investigators has been developed and made available for individual forces to use. Cybercrime modules have been developed and are being introduced nationally into all IPLDP (Initial Police learning and Development), ICIDP (Initial Crime Investigator’s Development) and Senior Investigating Officer programmes. Additionally the College of Policing has developed a Mainstream Cybercrime training course for investigators, which North West forces are preparing to deliver or have begun delivery of. It is anticipated that investment in this training will greatly enhance the knowledge of mainstream investigators in cybercrime and its investigation across the North West region.

All North West forces are experiencing difficulty in establishing the true scale of cybercrime in their respective force areas, which in turn makes identifying the regional problem difficult. Forces are exploring how to introduce a crime recording flag for cyber enabled / dependant crime which will present a more accurate picture of the cybercrime landscape. This is not a problem unique to the North West area, it is recognised that nationally the police lack the reporting and data-mining mechanisms to capture accurate data on the varying forms of cybercrime (ACPO, 2013).

Good practice is evident amongst North West forces that are making effective use of inviting academic students into cyber and e-forensics units. This provides valuable opportunities for students to complete work-based placements as part of their degree programmes and in turn provides enhanced capacity and capability in those units.

Whilst it is evident that all North West forces have the capability to deal with cyber enabled crimes (traditional crimes which have been transformed in scale or form by the use of the internet) utilising the skill sets that are held by officers and staff working within different departments, forces are less confident in their ability to deal with cyber dependant crimes (those where the digital system is the target as well as the means of attack) and therefore investigative support for such investigations is often obtained from the North West Regional and the National cybercrime units.

There is a general acceptance across forces that the investigation of such offences requires significant capital investment and investigators to acquire a new skills set which often transverses many of the other skill areas (for example, Open Source, E-Forensics, Communications Data investigation). The ability to proactively target those committing cyber related crime is presenting challenges for North West forces and all agree that there is a need to gain a fuller picture of how cyber criminals are operating in and impacting upon the North West police region. Recognising the need for dedicated cybercrime investigation teams that are capable of investigating cyber dependant offences North West forces are exploring the options available to them to meet this demand, one option being considered is regional collaboration.

# Defining Cybercrime

Cybercrime has been an elusive concept and one of much debate during the workshop. Discussions ranged from focusing on operational definitions all the way through to high level academic descriptions. Just as important as defining what cybercrime is, is what it is not. There was considerable concern that anything that involved some form of technology was now being considered a cybercrime. These concepts were brought out during the group workshop sessions that will be discussed in detail later in this report. A prevalent concern was that without accurate and appropriate definitions, cybercrime, and wider crime statistics would not be accurate.

David Wall in his 2007/10 article, identifies three generations of cybercriminal activity:

* Crimes in the machine (computer content)
* Crimes using machines (computer related)
* Crimes against the machine (computer integrity)

Wall also identifies a future where the offender victim interaction is automated by technology completely removing the need for victim selection and interaction. These classifications provide a useful framework for evaluating the evolution of criminal activity as mediated by technology. However more commonly government agencies, law enforcement, businesses and academics tend to utilise two categories to define cybercrime, commonly defined as:

**Computer enabled crime:** traditional crime that is increased in its scale, reach or impact through the use of technology. For example, phishing which attempts to acquire details (i.e. bank details) through email by purporting to be from a legitimate organisation as opposed to an individual eluding to be the gas man to retrieve bank details.

**Computer dependent crime:** crime which could not exist without new technology. For example; harvesting bank account details through malware.

As we shall see later in this report there is also a need to distinguish between cybercrime and digital evidence. It is entirely possible that any crime may have some associated digital evidence, and yet that crime may not be a cybercrime. However, by the very nature of cybercrime in that it uses information technology, it must have digital evidence. This distinction is important in order to be able to make considered resource allocation for law enforcement and also for crime reporting. It also plays to the concern that anything connected to the internet is considered a cybercrime.

While it is possible to build an analytic framework and taxonomies for the classification of crimes, it will only be when they are used in practice will a complete picture emerge. As such it would be worth considering how the experiential learning of categorising criminal activity is reflected back within a constabulary and more broadly between constabularies and the agencies such as the NCA and the NCCU. Such a mechanism is perhaps the only way to deal with the rapidly evolving nature of technology and its use in criminal practice.

Survey Findings

During the event a proportion of the delegate were requested to complete a brief survey covering their experience and understanding of cybercrime. The purpose of this survey was to gather important information in regard to the baseline of understanding and perceptions within the audience.

While having suitable knowledge regarding cyber criminal activity is essential, what is equally important is the perception by individuals of what is and is not a cybercrime, beyond the relatively academic descriptions of Computer enabled and Computer dependent as identified earlier. The reader should be clear that the survey response rate is not large enough to be able to draw significant quantitative conclusions. However, it does provide an indicative impression of the audiences perception and adds weight to much anecdotal evidence. Further, more substantial research should be conducted to obtain a fuller picture.

# Experience of Cybercrime

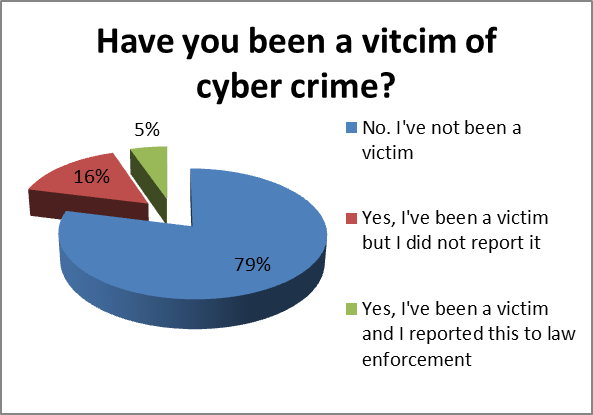
The audience undertaking the survey was, due to the nature of the event, biased towards the Law enforcement community – **68% of respondents**. When asked whether they had a mechanism to specifically capture and report cybercrime only **53% of the respondents indicated they had a cybercrime reporting system**. This identifies that some members of the law enforcement community are not fully aware of the cybercrime reporting capabilities that might be available to them. When asked specifically about the suitability of the available system **only 31% of the respondents felt that the cybercrime reporting facility was fit for purpose.** When asked if they had experienced cybercrime 79% indicated they have not suffered an incident, shown in Figure 1 which is unsurprising given the population in the audience. Importantly of those that did suffer an incident the majority did not report it. When probed further regarding the quality of the response given by the authority reported too, the overall impression was that the response was less than satisfactory.

Figure 1 Have you been a victim of cyber crime?

These results provide a small snapshot of the views of the audience in relation to cybercrime. They highlight a number of key issues and raise important questions that need to be responded to going forward. The first of these is to understand how the existing crime reporting systems, including those that are specifically there to support cybercrime reporting, work together to facilitate cybercrime reporting. A suitable paradigm here could a rigorous SWOT approach conducted at a regional basis with periodic reviews. Building on this understanding the cybercrime reporting approaches need to be communicated more within the Law Enforcement community. Specifically, pathways for external organisations and individuals need to be identified to enable external reporting of cyber criminal activity. The effective collection of information from external parties is vital to effective cybercrime policing due to the fact the space being policed, i.e. cyber space, is not a public environment, it is privately owned and operated. Therefore, co-operation from these private ‘cyber-land owners’ is essential. Following on from engagement leads on to ensuring that what is currently in place is fit for purpose. The analysis of the current systems and how they integrate will provide the foundation for this.

# Perceptions of cybercrime

As discussed an important consideration in understanding cybercrime is people’s perceptions of what a cybercrime actually is. The academic descriptions given in the previous section is useful for giving us a way to classify criminal activity, but it is important to understand how people would classify criminal activity. This is particularly important for Law Enforcement agencies when they have classified the criminal activity during arrest and prosecution. It has long been suspected that cybercrime has been under-reported with one a potential reason for this identified as a lack of clarity around how to classify cybercrime. The results in the following graphs are based on the responses from 19 individuals.

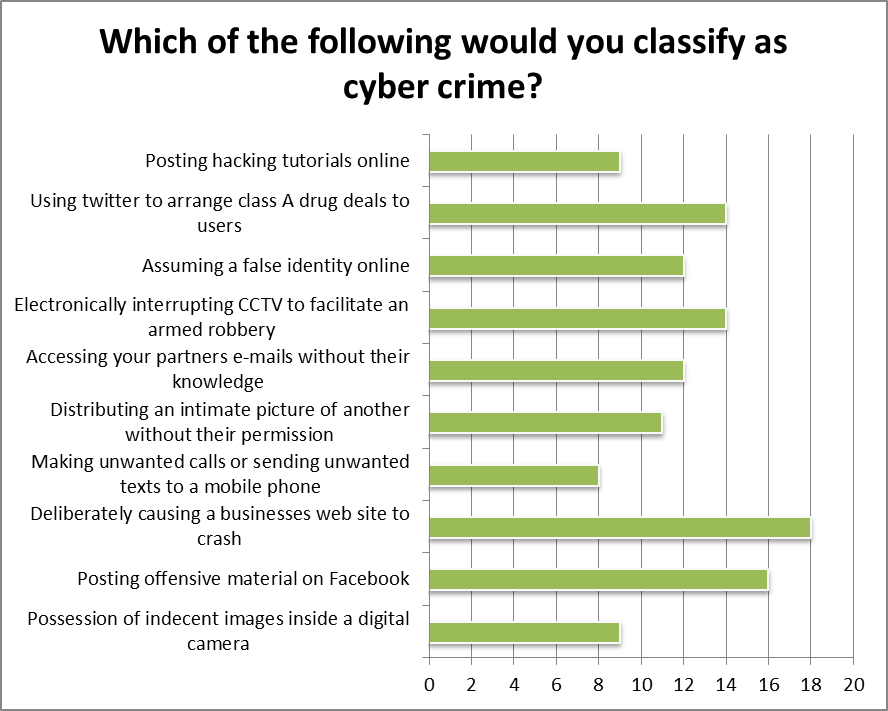


Figure 2 Which of the following would you classify as cyber crime?

The respondents were first asked whether they would classify a number of activities as a cybercrime with the results shown in Figure 2. What is important to note is that are no right or wrong answers as there are very few specific laws that define cybercrime and as highlighted those that do exist focus primarily on computer dependent crime such as the computer misuse act. In fact the acts identified were deliberately defined such that they identified a criminal act that incorporated some level of technology use. As can be seen from the results the majority of the respondents felt that all the acts would be classified as a cybercrime. One interpretation of these results is that there is considerable ambiguity over the distinction between a cybercrime and crime that has digital evidence. For example, consider “Using Twitter to arrange class A drug deals to users”. Twitter was only launched in 2006 and as such drug deals must have utilised other communication means to arrange deals. The use of Twitter in this case represents an opportunity to gather digital evidence to support the criminal case against the dealers in the same way that call records or telephone recordings would have been. The pertinent issue here is that **crimes may have digital evidence, but not all crimes with digital evidence are cybercrimes**. Importantly further work to be able to draw the line between these concepts and educate the wider audience will be vital going forward. The concept that digital evidence may be part of any criminal investigation has important resource ramifications, in terms of allocation and specialisation.

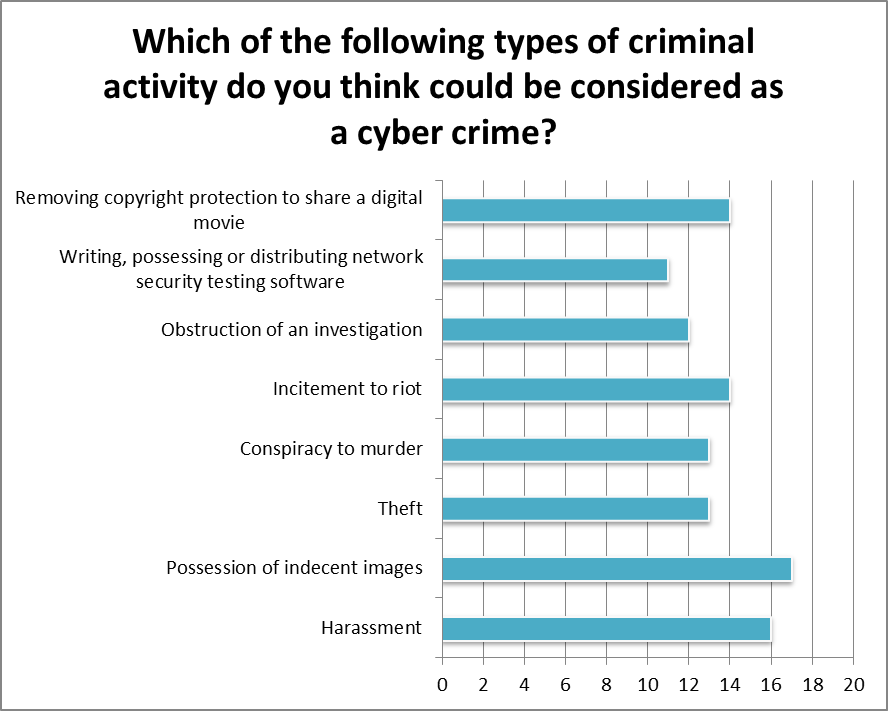


Figure 3 Which of the following types of criminal activity do you think could be considered as a cyber crime?

Following on from the previous results Figure 3 highlights how well defined criminal acts are often perceived to be cybercrime. For example, consider the possession of indecent images and harassment. Both of these have supporting legislation in their own right, however, common modes to preform these criminal acts often involve the use of technology and so in modern society have become synonymous with cybercrime. Interestingly the criminal act: “writing, possessing or distributing network security testing software”, is one that can fall directly under the computer misuse act and is the only one that could be consider as a computer dependent crime. Yet it is this criminal act that has the lowest number of votes.

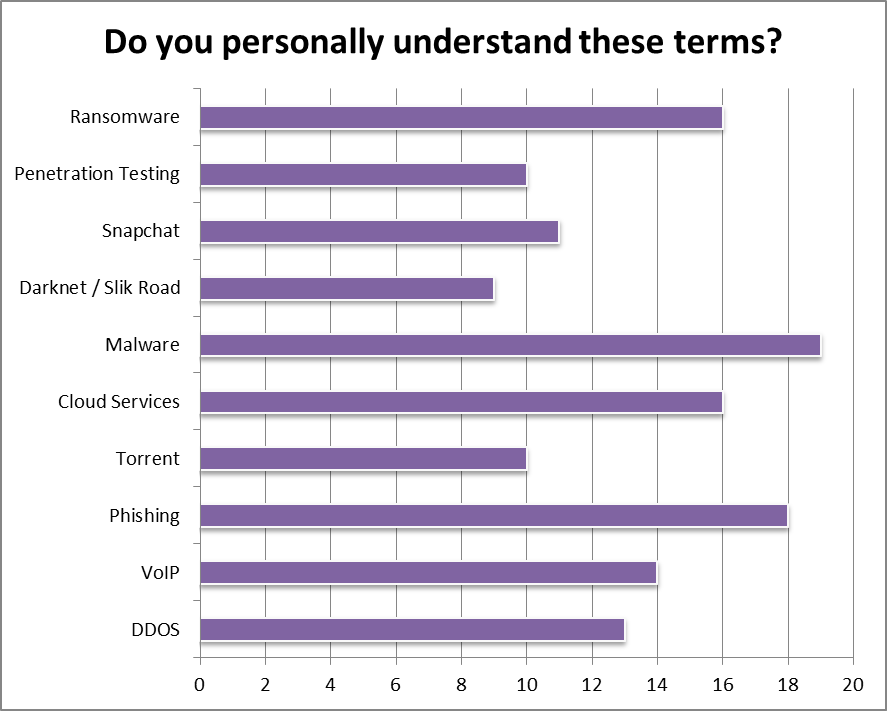


Figure 4 Do you personally understand these terms?

An important factor in people interpreting whether an act is a cybercrime is an understanding of technology and its uses. As such the survey attempted to capture whether the respondents understood technological terms. Again there are some methodological issues with the approach taken as this is a qualitative self-assessment process which in a more rigorous approach would be backed up with a further exploration of the understanding of the technical details to validate respondent assertions of understanding. At a very high level the results, given in Figure 4, speak to the variability of understanding across the respondents, which is to be expected. However, the response in dealing with the variation is needs to be carefully considered.

By its nature IT and its uses requires specialisation and constant emersion in order to stay on top of its uses for criminal purposes and also interpreting the data to provide forensic evidence. Any yet this is counteracted by the fact that technology is ubiquitous and woven into the fabric of society. Therefore a careful balance must be struck between how to resource the specialist activity and a wider programme to disseminate information about technology and how it may be used to support cybercrime and for that matter wider criminal activity.

# Cyber Pledge Analysis

During the workshop some of the delegates were asked to participate in a simple activity to undertake “cyber pledges”. The concept is to ask individuals to identify one small thing that they could do to help improve the cyber security of themselves or those around them. The purpose of the exercise is twofold. First, it is an effective mechanism to break the area of cyber security in to more manageable and operational chunks of achievable activity as cyber security can be seen as too large a problem to tackle. There is also a considerable amount of evidence that just getting the basics right drastically improve overall security. This acts as a mechanism to encourage that behaviour. An achievement on something small will build confidence to tackle larger issues. Second, it can be used as a source of intelligence in regard to the types of issues that people are facing on a day to day basis. This can then inform the provision of targeted rolling support and advice.

The collected pledges are listed in Appendix A. A basic qualitative analysis of the pledges reveals that the majority of them are to do with helping to educate and inform those around them either at work or at home. These statements are often correlated with a need to first gain the right information for distribution. This indicates there is a need to provide suitable information sources in a digestible form that can be used to help those individuals education and inform others. A further area identified was around collaboration and forming collaborative partnerships to help tackle the issues that are presented by cybercrime. This highlights two functions that a regionally co-ordinated activity could support; developing a consistent set of educational resources to inform a wider audience based on the regionally prioritised threats; Providing a mechanism to facilitate networks of practitioners in the region.

Working Group Findings

The main body of the workshop was formed by two discussion sessions where moderated groups discussed key questions that were intended to help illuminate the activities and relationships between all the interested stakeholders. During each session the moderator stimulated discussion and recorded the salient points. More than one group was asked the same question, enabling a broader range of responses.

# Monitoring and Measuring Cyber Criminal Activity

A key topic of discussion was exploring how the Forces and ROCUs should monitor and measure the threat from cybercrime. This is a key problem as crime figures underpin the allocation of resources, at both force level and regional level, to tackle the level of threat from a particular class of crime. Beyond Force and ROCU interaction, how to feed this information in the form of threat assessments between Forces, external partners and other agencies such as the NCA was considered. As identified earlier in this report, a common framework to enable this information exchange needs to be enacted. While the mechanisms for information exchange do exist, it would appear that definitions of cyber-criminal activity are fragmented and relating an arrest offence to an actual cyber offence is not common place or simple to achieve. It is therefore vital moving forward to provide a common language, leveraging existing approaches, accompanied by a simple and easy to understand approach to classification. Moving beyond this foundation, any such framework must also capture the offender and victim profiles in order to develop accurate threat intelligence approaches; potential high risk victim groups and well understood threat agents.

Given such a capability it becomes possible to undertake environmental scanning to identify threats to specific groups. However, should this be done at a regional level or at a force level? This type of intelligence analysis and dissemination was identified in discussions regarding the roles and responsibilities of a regional activity. That is not to say a Force level such capability is not required, in fact the ability to localise such threat information was recognised as vital to enhance the prevention activity in this space. However, it is important to recognise that the forces, ROCU and NCA may not be the only organisations that hold vital data on criminal activity. Considerable data regarding malicious acts may be held by third parties such as credit card companies or online market places. The intelligence that could flow from such organisations, which may operate globally via the Internet but need to be physically located within a Force area, would greatly enrich the threat assessment process. A regional hub could be ideally positioned to act as a single point of contact for such organisations. Similarly the reverse is true, such a regional hub could act as a vital threat intelligence dissemination point. To be clear, such a hub would need to add value in terms of intelligence and threat analysis, rather than merely be a gateway to information. This approach is in line with current approaches in regard to threat assessment that current local forces follow and provides an effective decision making process by risk and threat across policing problems. However, this local approach does need to be extended through some form of regional co-ordination due to the distributed and inherently non-geographical nature of cybercrime.

An important aspect of what has been outlined previously is the way approaches to tackling cybercrime are measured in terms of public opinion and satisfaction. Limited information is available on this, for example the crime survey for England and Wales contains few questions on cyber-crime. Therefore, it is difficult to assess the current public opinion on the matter beyond that which is reported in the mainstream media. In order to combat this it will be vital moving forward to provide a robust evidence based dialog with the general public in order to identify such outcomes as prevented activity and the impact on local communities of cybercrime. Importantly, ensure that victims of cybercrime are dealt with suitably including ensure that they have been listened to and that there was a suitable and proportional response. These activities could be effectively combined with approaches to localise the threat assessment information coming through from any regional activity.

Moving beyond measuring the public perception of the response to cybercrime is monitoring the efficacy of approaches against reported crime. The only way to achieve this is first to have a well understood and universal mechanisms to classify and report cybercrime, as discussed. Only by having appropriate metrification of cybercrime reporting will the efficacy of interventions (preventions, arrest and prosecution etc) can be measured. Here the distributed nature of cybercrime creates significant issues. Typically a traditional crime will affect the geographical areas in which it is commissioned. However, cybercrime often has a detachment from the criminal, the commission and the impact. For example a criminal in one Force area, may utilise a compromised computer remotely in another force area to impact a victim in a third force area. Additional consideration must be given to the easy with which criminals can move their cyber operations. Therefore, it is highly likely that certain interventions may cause significant displacement of parts of the criminal activity to a different force area. As a result a co-ordinated approach is needed to understand the impact of the intervention and any resultant displacement. This also calls into question the efficacy of regional or force area crime statistic reports due to the significant distributed nature of the cyber criminal act.

# Defining Local and Regional Capacity

While measuring and monitoring cybercrime is an important activity, it is vital that forces are able to respond locally and regionally, with the capability to hook into national and international activities. However, in order to do that appropriate capability needs to be established around technical a range of new and specialised capabilities. Therefore, the attendees were asked to define the remit for a regional cyber unit and force cyber units and further consider the tasking process for each unit.

Generally it was felt that any regional-local structure should focus on a preventative strategy as it was identified that around 80% of cyber security vulnerabilities could be tackled through basic user education and awareness. However, it was identified that there needs to be a clear understanding of the threat level that individuals are exposed to. This fits with the previously outlined intelligence agenda that such a regional-local structure could facilitate. The issue of effective resourcing was highlighted here and how support for this preventative activity fits with local priorities that maybe set by Police and Crime Commissioners and any Home office initiatives. Here, the role of intelligence gathering may provide an effective solution. With a strong evidence base of the level and impact of cyber criminal activity it supports a more coherent discussion around resource allocation, not just for preventative action but a whole range of responses, balanced against allocations to deal with other areas of response.

One vital process that needs to be well defined is the mechanism by which activities such as investigations or forensic examination move between regional or local units. This will be largely dependent on the capabilities found in the local force units and any regional unit, coupled with the nature of what is being moved. Here it should also be considered that activities may not be moved to the regional unit, but may be moved to another force cyber unit that has developed the necessary capability to tackle a specific localised threat. Here the role of the regional unit as a network facilitator comes into play and may also require the regional unit to have some form of capability to ensure operational transition between force units and/or force-regional units. It was generally difficult for the working groups to develop a clear tipping point between what should be a regional or force unit activity and what the transition point should be. Here it would be advisable to leverage existing operational practice for handling organised or complex financial crime. Regardless, care must be taken to ensure that the processes are well defined and that the process definitions ensure that, as far as possible, all conditions for transfer are considered. To be clear, this also involves the transfer of investigations from any regional unit to the local unit as well. Potentially, expertise around the design and implementation of High Reliability Organisations (HROs) may be beneficial in defining the operational procedures. Specifically care should be taken in considering transfers during different levels of operational tempo. For example, consider the transfer process needs if a regional business is currently under cyber attack as opposed to that same business being identified as a potential target.

## Force Characteristics

In discussing the nature of a force cyber unit, it is important to draw the distinction between handling and processing digital evidence and the investigation of cybercrime as highlighted earlier. The handling of digital evidence will be vital to all police forces going forward as more and more digital technology is used in the commissioning of criminal acts. However, the ability to process, handle, interrogate digital devices for information pertaining to an investigation does not make that investigation itself inherently cyber. It would therefore, be more appropriate to consider two separate units, one to handle digital devices and the evidence obtained from it, and one that has the specialist ability to investigate a cybercrime. While there needs to be a common technical capability between both units, it would be reasonable to consider both units as separate as those that specialise in crime scene investigation and those focused on complex financial crime.

Consider for a moment the digital forensics capability. Here it was felt that the Force units should be equipped to handle standard, widely used digital equipment. This capability will help to underpin any type of investigation. Beyond this such a unit should be able to support cyber investigations that involve the use of common off the shelf “crimeware” technologies. Therefore these forensics units should be able to accommodate:

* Technical Triage: The ability to handle common technical situations and provide advice into investigations
* Front line Forensics support: The ability to handle common digital forensic scenarios, in a similar vein as physical crime scene investigation capability
* Intelligence gathering: The ability to be able to gather routine information regarding trends of criminal activity and their use of technology.

The final point regarding intelligence is vital in order to provide a foundation for effective resource allocation and threat assessments, within the Force and at a regional level.

The Cyber Investigative capability should therefore focus on how the technology was used in the commissioning of the crime. While technical knowledge is needed, it is more important for those investigators that are specialising in cyber criminal activity that they understand the criminal, their link with the victim(s) and the motivation behind the crime. This separation in the capability is similar to that which is being seen in the cybercrime world. Traditionally, the person developing the malicious software would be the one using it to undertake a criminal act. Now however, groups of individuals are developing the malicious software and then criminals are using that software to commission a crime. Here, the thoughts are that there should be force specialisms in understanding the mainstream technology that is developed by malicious groups, which requires deep technical insight, and in understanding the criminal use of those technologies.

Regardless of the separation of these capabilities it was felt that the Force units should have a strong focus on providing local access points for the community in terms of local reporting and having someone to speak to in order to gain advice, fitting well with community policing approaches. These two streams of capability will have the localised knowledge, potentially augmented with information from other force areas as discussed previously, to be able to advise effectively the local community.

## Regional Characteristics

Given the outline force structure, it is important to understand the role of any regional activity. It was felt there should be two key fundamental capabilities that are needed in a regional capability that 1) map on to a similar capabilities in local forces 2) tackle the two key features of cyber criminal activity; wide scale distribution of activity and rapid evolution in the development of new technologies for the commission of crime. Mapping on to local force capability (investigation, forensics) provides continuity of function and job role, to create flexibility in secondment and support. However, the regional capacity should focus on delivering capability that benefits from centralised and consolidated work, typically a focus on high tech and emergent technologies.

Therefore, it was identified that a high tech capability should be retained at the regional level to tackle the rapid evolution of technology. The appropriate response here is to provide technical specialisms that are able to tackle never before seen technologies or uses of technology. Here, it was felt that this technical capability should really focus on what would be considered computer dependent crime. An important aspect of this that came across was not only understanding the technology, how it works, what evidence can be recovered and so on, but the way criminals are using the technology. Technology use profiles could form an effective mechanism to help inform investigations.

The distributed nature of cybercriminal activity requires a co-ordinated response that extends beyond traditional force boundaries. Therefore, it was felt that a regionally co-ordinated activity is a vital part of an effective response in a similar way to that required for organised crime. Such a regional capability would be supported by the previously identified vital regional capability of intelligence processing and providing an access point for other key organisations such as geographically located large industry or the NCA/NCCU. This combination would facilitate effective regional horizon scanning of threats.

Beyond these core activities, it was felt that it would be very useful for a regional capability to provide consolidated co-ordination in a number of logistics areas relating to cyber-policing. These include:

* Regional co-ordination of consolidated buying. This would reduce overhead in commissioning operational capability while the commonality in operational capability would simplify training and knowledge and evidence exchange.
* Training provision. Acting as a hub to provide training to local forces on both technology and investigative capability.
* Co-ordination of specialisms and capability. While it has been identified that forces need to have general technical and investigative capability, some forces may need to specialise in specific areas in order to combat a specific threat profile with in their geographical region. A regional activity could provide oversight and co-ordination to ensure transfer of best practice and facilitating collaboration for specific investigations.

# Regional Support

Building on from the identification of which capability should be established at a local and regional level, the attendees were asked to consider what a specialist ROCU cyber unit should look like to facilitate the effective delivery, at a regional level of harm reduction, prevention and enforcement. Further, the attendees were asked how the region should organise itself to deliver this and what opportunities there are for regional collaboration.

By and large it was recognised that the nature of cybercrime created a need for high-tech specialisms in addition to the need for intelligence gathering/processing and co-ordination of geographically broader and more organised crime investigations. This focus on high-tech specialisms also leads to a more focused effort on what we have termed computer dependent crime, that which can only exist with a computer. It will be vital for the any central unit developing these skills and knowledge is passed to local forces as that technology becomes more wide spread in criminal use. It is therefore worth considering how this information is feed into force units to follow trends in technology use for crime. Specifically it is worth identifying clear benchmarks that would trigger such dissemination. A balance needs to be maintained for any central unit between retaining skills and knowledge and facilitating its dissemination.

One key concern is the potential conflict between the way police service operates in terms of secondments and the need for long term specialism development to deal with the rapidly evolving nature of the technology used to commit cybercrime. It is widely recognised in industry that it takes an individual around 3 to 4 year to become a cyber security specialist. It is reasonable to expect a similar time frame for with a digital forensics specialist or a cyber investigator. Therefore, at the point at which an officer gets to the right level in their chosen field they may be moved. It will therefore be vital that the career pathway and retention of staff be considered carefully within the local and regional force structures to ensure there are proper incentives for individuals to invest in developing and retaining these skills.

Beyond these concerns the secondment mechanism could provide a strong foundation to underpin exchanges of skills and knowledge between any regional unit, local cyber units and more widely within local forces. Here consider short term secondments on something of the order of six months to the regional unit. These, secondments could be coupled with a range of training, either delivered by the regional unit or other delivery partners such as academia. A rolling programme of training at a range of level could be delivered, from basic crime scene handling all the way up to detailed malware analysis and individuals seconded appropriately based on their skill sets. Not only would such a mechanism benefit the regional unit by increasing operational capability, and benefit local force staff by receiving training, it would also facilitate the creation of a strong network of cyber policing professionals. It has been demonstrated that networks created during such cohort training last long after the end of the training. This will therefore enable one of the key features that should underpin an effective regional and force cyber unit relationship built on partnership and interdependence. Specifically the notion that a regional cyber unit could act as an effective facilitator of a network of interconnected force cyber units.

Whilst so far this document has focused on developing a response to the uses of technology in the commissioning of criminal acts, a regional unit may also be in a position to explore how technology can be used to support investigations. This has already been covered in some part through the consideration of forensics capabilities. However, as new technologies are developed and deployed it is important to understand what intelligence may be obtained from them in order to support investigations and how, from a legal and technical perspective, such intelligence may be obtained. For example, what investigative intelligence can be obtained from the latest smart phone or social networking site? This is not reviewing technology for criminal use, but at technologies use in general. A strong ethical framework will be necessary to guide the implementation of such an approach. It is worth therefore reviewing existing ethical guidelines and seeing what can be leveraged and what needs to be developed to cover this activity.

# Intelligence Led Cyberpolicing Innovation Ecosystem

It is vital that law enforcement is able to keep up with the rapid advances in technologies and particularly their use within criminal acts. However, it is not feasible for law enforcement agencies to do this by themselves. There are numerous and various reasons for this including resource constraints, the wide variety of priorities that the agencies must deal with and so on. It therefore becomes essential for agencies to work closely together and look beyond their traditional collaborators.

Cybercrime and cyber security is by its very nature an innovative and creative act. Individuals and groups take existing technology, develop it or augment it in ways that the technologies originators may have never envisioned. Further these individuals are adept at drawing on internal and external ideas and knowledge to advance technology for their use. Law enforcement agencies must therefore adapt in a similar way to be able to draw from the best internal capability and combine that with the best from legitimate external groups. It is clear from the discussions presented in this paper that collaborative and dynamic approaches are needed in order to provide an effective response. Not only is the nature of the threat and the way the threat operates (using new malware and exploits) changing, but also the nature of the environment that criminal can take advantage of is changing, considered the rapid adoption of smartphones or the introduction of tablet computing. Given this context and that of multiple parties holding relevant information regarding criminal activities, new models of interaction are needed.

In some ways the agencies should adopt the concept of Open Innovation as promoted by Henry Chesbrough. This model calls for organisations to work collaboratively to drive innovation by sharing risk and reward. Within law enforcement the concepts around risk and reward are very different to those in the commercial sector. However the flow of ideas and collaboration present in this model provide one potential solution for those agencies tasked with the protection of the peace and crime prevention to tackle in innovative ways the challenges that cybercrime and policing present. By using such a model to underpin collaboration, coupled with well understood risk-reward trade-offs, a new cyber policing innovation ecosystem could be developed. In such a model key parties are able to:

* More freely exchange information; boosting intelligence of criminal activity in terms of acts, victomology and offender profile,
* Exchange ideas on solutions; taking advantage of cutting edge research
* Leverage key specialisms that the nature of cybercrime demands; specialisms in forensics for mobile phones

A model of this interaction is given in Figure 5. Here we can see the interactions with the potential lists of key stakeholders and how solutions and opportunities might flow between them. On the left the intelligence on the cyber threat circulates between the key stakeholders in order to generate a rich pool of information upon which to draw upon in order to identify where to invest resources to tackle the greatest threat. On the right, the figure show how that intelligence may be turned be transformed into niche research and then operationalised via collaboration with a range of commercial partners. Therefore, this model has the potential to generate two key impacts, reduction in harm and loss prevention, and delivering economic growth through the creation of new commercial products and services.

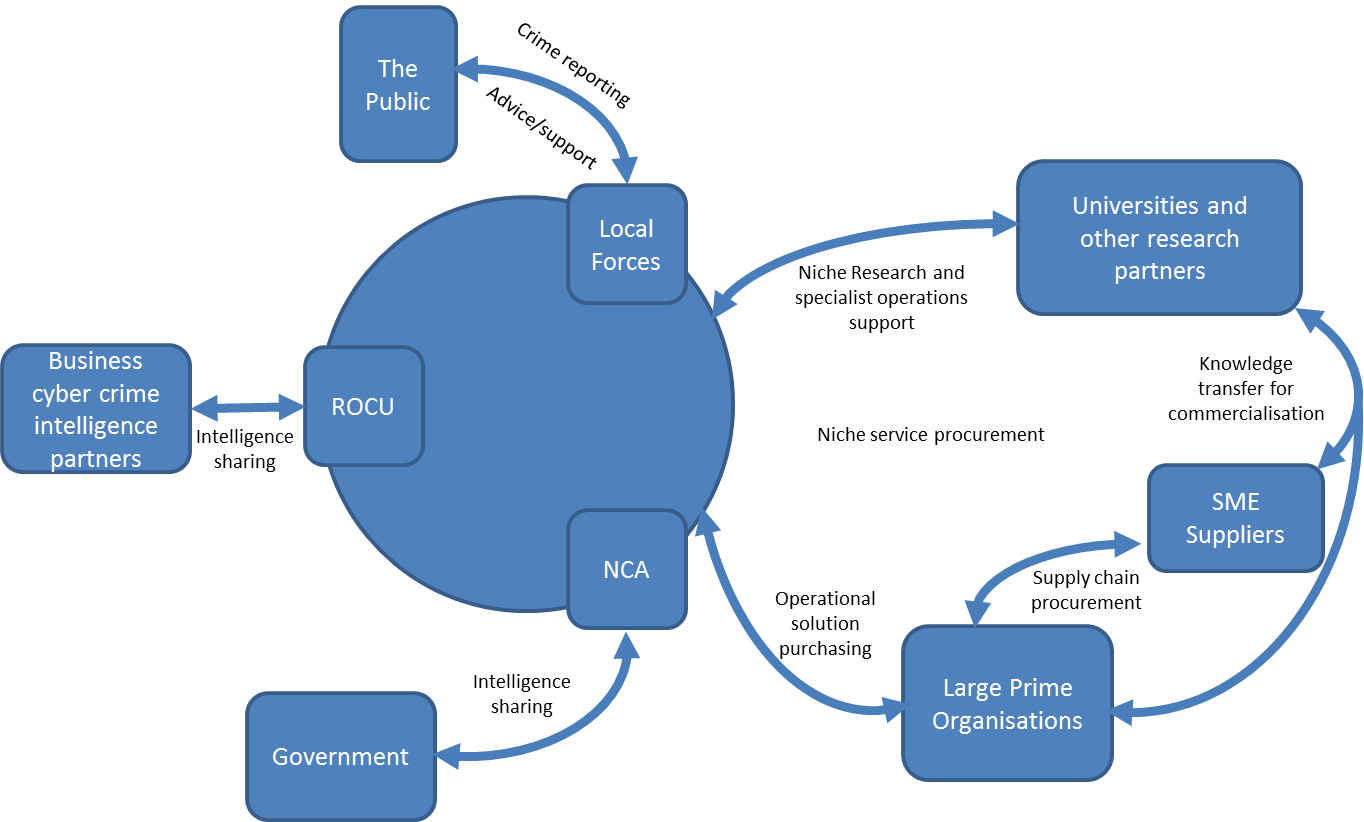


Figure 5 Intelligence Led Cyber Policing Innovation Ecosystem

Conclusion

Cyber policing presents significant challenges due to the rapidly evolving nature of the technology and its use in criminal acts, the pervasive nature of technology and the fact that the “space” that is being policed is largely held in private hands. This presents an interesting environment where policing and public order activities interact directly with capitalism and business decisions. This report has brought together key views and thoughts on how the North West should actively tackle this growing threat in a positive manner to protect the community.

This report highlights the need for cyber crime reporting mechanisms to be reviewed and enhanced, a number of NW forces have no clear reporting / recording system for cyber crime and almost 2/3 of delegates felt that cyber crime reporting mechanisms we not fit for purpose. Under the current system relating an arrest offence to an individual it not always achieved and assessing the efficacy of interventions is difficult to measure. It is recommended that a SWOT analysis is conducted of the existing cyber crime reporting systems and that they are developed to ensure that there is clear and effective reporting mechanism via which individuals and industry can report cyber criminal activity which will ensure the effective collection of information and intelligence from external parties.

Even amongst law enforcement there remains considerable ambiguity over the distinction between a cyber crime and a crime that has digital evidence. Without clarity and consistency the credibility of crime reporting and recording statistics will be questionable. A new framework and a clear set of guidelines needs to be established which will also capture offender and victim profiles to ensure that accurate threat analysis and assessment can be conducted and high risk individuals, companies or groups can be identified and the threats clearly understood. Those involved in crime recording and analysis require educating on any revised framework and procedures.

There is an important difference between a cybercrime, or cyber criminal activity and the use of digital evidence. It is highly likely that a criminal investigation today will include some form of digital evidence, for example call logs, or images captured on a smart phone. However, the use of digital evidence does not necessarily lead to the criminal act being classed as a cybercrime. Therefore a key principle is that all cybercrimes by their nature will generate digital evidence, but having digital evidence does not mean a cybercrime has been committed. It therefore follows that a cybercrime unit should not be solely responsible for a digital forensics capability. In fact the support for digital forensics should arguable be made available to any criminal investigation that requires it and put on a footing with other investigative forensics services. Similarly cybercrime investigation is a very specific skill set backed up with knowledge about how those cybercriminals operate. Parallels may be drawn here to organised crime, or other types of specific criminal investigation, such as complex fraud. Therefore, a cybercrime investigation teach do not need to be experts in digital evidence, but experts in how cyber criminals operate and the techniques and tools they use.

The gathering of information and intelligence from non law enforcement agencies is vital and more needs to be done to ensure that it is effectively and accurately gathered. It is recommended that a regional hub would be ideally positioned to act as a single point of contact for such organisations to not only gather, process and add value to intelligence but to also act as a vital intelligence dissemination point.

There is a desire to improve the standard of cyber crime awareness and prevention advice that is available and given. Suitable information sources which are in a digestible form that can be used to educate and inform individuals and organisations should be acquired or produced.

There is a need to improve the service provided to the victims of cyber crime to ensure that they get a suitable and proportional response and that there is consistency across force boundaries. The provision of a robust evidence based dialogue with the public will be vital to ensure that cyber crime prevented activity and community impact is accurately assessed and managed.

It was generally agreed that there is a need for greater collaboration and partnership working to effectively tackle the threats posed by cyber crime, a key element of which is the relationship between force cyber crime investigation capabilities and those regionally based. It was concluded that the relationship should be one of partnership and interdependence rather than the development of a strict hierarchy with the regional team acting as an effective facilitator of a network of interconnected force cyber units. Concern was raised that in regional forces the need to maintain front line resources would take priority creating a reluctance for investment in regional cyber crime units and that smaller forces may actually get more out of the contribution than larger ones. Local forces need to build skills and expertise to investigate the broad range of cyber crimes and regional cyber crime units should act as the professional head. The regional unit should be a hub for capturing and coordinating cyber crime related data and sharing information about emerging threats, tactics and technologies with forces and industry. It was suggested that a minimum of 10 staff would be needed which would need to include individuals with skill sets covering E-Forensics, competent investigator, covert internet investigation, advanced disclosure and data analyst.

Appendix A - Pledges

* I have already made a formal presentation to the DCC responsible for quality and customer satisfaction and explained the impact of fraud and now Cybercrime and its impact on victims. Has it worked however? ACPO need to feel the pain.
* I pledge to make the busiest shopping day of the year the safest online by raising awareness among the population of the dangers of cybercrime.
* I pledge to update my online security and raise awareness of the scale of issue with my colleagues.
* I pledge to put together (or more likely find online) a security check list, apply it myself and distribute it to my students.
* I pledge to work with others in SE region to create an effective cyber investigation capability for the region.
* I pledge to build a regional cyber capability within London, through good working relationship / collaboration.
* I pledge to try and enlighten family, friends and colleagues of the need to be alive to the cyber risks that exist.
* I pledge to engage more with academic and other businesses.
* I pledge to shred old credit card bills, gas bills etc.
* I pledge to check my own software security! Design a ROCU cyber unit that is best fit with forces and NCA.
* I pledge to develop an effective regional cyber capability for the North West region.
* I pledge to promote cybercrime within North Wales at a strategic level.

Authors

**Dr Daniel Prince: Associate Director of Partnerships at Security Lancaster**

Daniel Prince is an associate director for Security Lancaster, managing business partnerships and enterprise. Prior to this he was the course director for the multi-disciplinary MSc in Cyber Security teaching penetration testing, digital forensics and information security risk management. Daniel holds a PhD in Computer Science and has worked on projects with numerous large technology companies such as Cisco and Microsoft.

**Catherine Elvey**

<TODO>

**Janet Hudson**

<TODO>

References

Farrington, D.P. (1992). ‘Criminal Career Research in the United Kingdom,’ *British Journal of Criminology,* Vol.32, No.4.

Francis, B., Soothill, K. and Ackerley, E. (2004). ‘Multiple Cohort Data, Delinquent Generations, and Criminal Careers,’ *Journal of Contemporary Criminal Justice*, Vol. 20, No.2, May, 103-126.

Holt, T. J. (2010). Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data. *Journal of Criminal Justice Education*, Vol.21, 300-321.

Holt, T. J., Soles, J., and Leslie, L. (2008). Characterizing malware writers and computer attackers in their own words. Paper presented at the 3rd International Conference on Information Warfare and Security, April 24-25, in Omaha, Nebraska.

Holt, T.J., Strumsky, D., Smirnova, O. & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology,* Vol.6, No.1, 891-903.

Macloed, J.F., Grove, P.G. and Farrington, D.P. (2012). *Explaining Criminal Careers: Implications for Justice Policy,* Oxford: Oxford University Press.

Soothill, K., Fitzpatrick, C. and Francis, B*.* (2009). *Understanding Criminal Careers*, Devon: Willon Publishing.

Wall, D.S. (2007/10).Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (Revised May 2010), *Police Practice & Research: An International Journal,* Vol.8, No.2, 183-205.

**TITAN**, the name for the North West Regional Organised Crime Unit, was established in 2009 as a collaboration between the six police forces in Cumbria, Cheshire, Lancashire, Greater Manchester, Merseyside and North Wales to tackle serious organised crime that crosses county borders in the region. The mission of the unit is simple - to tackle organised crime groups causing the greatest levels of harm to communities in the North West. The unit is comprised of five teams working closely together and includes representatives from Her Majesty's Revenue and Customs, UK Border Agency and the National Crime Agency. Those teams are: the Regional Intelligence Unit (RIU), the Regional Crime Unit (RCU), the Regional Asset Recovery Team (RART), Regional Cyber Crime Unit (RCCU) and the Protected Persons Service Unit (PPS).

**Security Futures’** mission is to is create a space where we could develop innovative techniques to think about the future, techniques that draw together the insight and expertise of researchers working across different disciplines. In this collaborative space, researchers and other partner organisations have the freedom to explore questions about security and technology. But also to formulate the questions that we might need to start asking about the emerging trends in technology, society and security. A space where we can bring together people working on the cutting edges of technology, social, legal and political disciplines to ask questions about the world we live in. A space where we might begin to imagine new horizons and start to see the problems that

**Security Lancaster** is a university wide research centre on security and protection sciences. It delivers research and education that innovates and creatively challenges the way that individuals, organisations and societies secure and protect themselves. This is achieved via engagement and collaboration with organisations from a range of sectors along with governments. The centres approach delivers the very best use-inspired and pure research alongside cutting edge education that delivers real impact and social change.

This work was funded by Security Lancaster via the auspices of Lancaster University’s Faculty of Science and Technology and by TITAN: The North West Regional Organised Crime Unit.

**Science and Technology Business Partnerships and Enterprise**

As well as working with a range of external partners, ICT and Security form part of a wider theme based team across Science and Technology at Lancaster who offer expertise in:

|  |  |
| --- | --- |
| * Advanced Manufacturing * Energy * Environment | * Health & Human Development * Quantum Technologies * Mathematics and Statistics |

**Working in Partnership**

Across the themes we form collaborative partnerships around these 5 key areas:

* Collaborative Research and Consultancy
* Training and Education
* Co-location and Secondment
* Student Placements
* Product Development and IPR

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Lancaster University, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Copyright Lancaster University ©2014